Volume 78, Number 90
Thursday, May 9, 2013
Public Notice 8314; Page 27276

Privacy Act; System of Records: Security Records, State-36.

SUMMARY: Notice is hereby given that the Department of State proposes to amend an existing system of records, Security Records, State-36, pursuant to the provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a) and Office of Management and Budget Circular No. A-130, Appendix I.

DATES: This system of records will be effective on June 18, 2013, unless we receive comments that will result in a contrary determination.

ADDRESSES: Any persons interested in commenting on the amended system of records may do so by writing to the Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW; Washington, DC 20522-8001.

FOR FURTHER INFORMATION CONTACT: Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW; Washington, DC 20522-8001.

SUPPLEMENTARY INFORMATION: The Department of State proposes that the current system retain the name "Security Records" (previously published as 72 FR 73057). The records maintained in State-36, Security Records, capture data related to incidents and threats affecting U. S. Government personnel, U. S. Government information, or U. S. Government facilities world-wide for a variety of legal purposes including Federal and state law enforcement and counterterrorism purposes. The information maintained in Security Records may also be used to determine general suitability for employment or retention in employment, to grant a contract or issue a license, grant, or security clearance. The proposed system will include modifications to all of the sections.

The Department's report was filed with the Office of Management and Budget. The amended system description, "Security Records, State-36," will read as set forth below.

Joyce A. Barr,
Assistant Secretary for Administration,
U.S. Department of State.

STATE – 36

SYSTEM NAME:
Security Records.

SECURITY CLASSIFICATION:
Unclassified and Classified.

SYSTEM LOCATION:
Department of State and its annexes, Bureau of Diplomatic Security, various field and regional offices throughout the United States, and abroad at some U.S. embassies and U.S. consulates.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Present and former employees of the Department of State; applicants for Department employment who have been or are presently being investigated for security clearance; contractors working for the Department; interns and detailees to the Department; individuals requiring access to the Department of State premises who have undergone or are undergoing security clearance; foreign mission members, international organization employees, domestic and household members to include private servants, and other foreign government personnel and their dependents accredited to the United States; some passport and visa applicants concerning matters of adjudication; individuals involved in matters of passport and visa fraud; individuals involved in unauthorized access to classified information; prospective alien spouses of U.S. personnel of the Department of State; individuals or groups whose activities have a potential bearing on the

security of Department or Foreign Service operations domestic and abroad including those involved in criminal or terrorist activity; suspects, victims, or witnesses associated with investigations into possible unlawful activity conducted by the Bureau of Diplomatic Security; visitors to the Department of State (the Harry S Truman Building), to its domestic annexes, field offices, missions, and to the U.S. embassies, consulates and missions abroad; and all other individuals requiring access to official Department of State premises who have undergone or are undergoing a security clearance. Other files include individuals issued security violations or infractions or cyber security violations or cyber security infractions; litigants in civil suits and criminal prosecutions of interest to the Bureau of Diplomatic Security; individuals who have Department building passes; uniformed security officers; individuals named in congressional inquiries to the Bureau of Diplomatic Security; individuals subject to investigations conducted on behalf of other Federal agencies; and individuals whose activities other agencies believe may have a bearing on U.S. foreign policy interests.

CATEGORIES OF RECORDS IN THE SYSTEM:

Incident and investigatory material relating to any category of individual described above, including case files containing but not limited to items such as: general physical description (including height, weight, body type, hair, clothing, accent description, and other general and distinguishing physical features); identification media (such as passports, residency, or driver's license information); email address; family identifiers (such as names of relatives and biographic information); numeric identifiers (such as Social Security numbers (SSNs), Employee ID numbers, State Global ID numbers (SGID)); applications for passports, drivers' licenses, residency and employment; photographs; biometric data; birth certificates; credit checks; intelligence reports; security evaluations and clearances; other agency reports and informant reports; legal case pleadings and files; evidence materials collected during investigations; security violation files; training reports; administrative files related to the implementation of the Foreign Missions Act, provision of services and benefits; administrative files related to the notification of appointment, termination of appointment and dependent employment requests for foreign missions members, employees of international organizations, domestic and household members to include private servants, and other foreign government personnel and their dependents accredited to the United States (elements of this category of records are maintained also by the Department's Office of the Chief of Protocol); weapons assignment data base; firing proficiency and other security-related testing scores; availability for special protective assignments; language proficiency scores; intelligence reports; counterintelligence material; counterterrorism material; internal Departmental memoranda; internal personnel, fiscal, and other administrative documents, including employee applications for diplomatic passports and visas. For visitors: name; date of birth; citizenship; ID type and ID number; temporary badge number; host's name; office symbol; room number, and telephone number. For all others: name; date and place of birth; home address; employer and employer's address; badge number; home, cellular, and office telephone numbers; SSN; specific areas and times of authorized accessibility; escort authority; status and level of security clearance; issuing agency and issuance date. For all individuals: date and times of

entering and exiting Department buildings. Security files contain information needed to provide protective services for the Secretary of State, other designated U.S. officials, resident foreign officials and facilities, and visiting foreign dignitaries.

There are also information copies of investigations of individuals conducted abroad on behalf of other Federal Agencies. Security files also contain documents and reports furnished to the Department by other Federal Agencies concerning individuals whose activities these agencies believe may have a bearing on U.S. foreign policy interests.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

(a) 5 U.S.C. 301 (Management of Executive Agencies); (b) 5 U.S.C. 7311 (Suitability, Security, and Conduct); (c) 5 U.S.C. 7531-33 (Adverse Actions, Suspension and Removal, and Effect on Other Statutes); (d) 8 U.S.C. 1104 (Aliens and Nationality—passport and visa fraud investigations); (e) 18 U.S.C. 111 (Crimes and Criminal Procedures) (Assaulting, resisting, or impeding certain officers or employees); (f) 18 U.S.C. 112 (Protection of foreign officials, official guests, and internationally protected persons); (g) 18 U.S.C. 201 (Bribery of public officials and witnesses); (h) 18 U.S.C. 202 (Bribery, Graft, and Conflicts of Interest-Definitions); (i) 18 U.S.C. 1114 (Protection of officers and employees of the U.S.); (j) 18 U.S.C. 1116 (Murder or manslaughter of foreign officials, official guests, or internationally protected persons); (k) 18 U.S.C. 1117 (Conspiracy to murder); (l) 18 U.S.C. 1541-1546 (Issuance without authority, false statement in application and use of passport, forgery or false use of passport, misuse of passport, safe conduct violation, fraud and misuse of visas, permits, and other documents); (m) 22 U.S.C. 211a (Foreign Relations and Intercourse) (Authority to grant, issue, and verify passports); (n) 22 U.S.C. 842, 846, 911 (Duties of Officers and Employees and Foreign Service Officers) (Repealed, but applicable to past records); (o) 22 U.S.C. 2454 (Administration); (p) 22 U.S.C. 2651a (Organization of the Department of State); (q) 22 U.S.C. 2658 (Rules and regulations; promulgation by Secretary; delegation of authority) (applicable to past records); (r) 22 U.S.C. 2267 (Empowered security officers of the Department of State and Foreign Service to make arrests without warrant) (Repealed, but applicable to past records); (s) 22 U.S.C. 2709 (Special Agents); (t) 22 U.S.C. 2712 (Authority to control certain terrorism-related services); (u) 22 U.S.C. 3921 (Management of service); (v) 22 U.S.C. 4802 (Diplomatic Security), 22 U.S.C. 4804(3)(D) (Responsibilities of Assistant Secretary for Diplomatic Security) (Repealed, but applicable to past records); (w) 22 U.S.C. 4831-4835 (Accountability review, accountability review board, procedures, findings and recommendations by a board, relation to other proceedings); (x) 44 U.S.C. 3101 (Federal Records Act of 1950, Sec. 506(a) as amended) (applicable to past records); (y) Executive Order 10450 (Security requirements for government employment); (z) Executive Order 12107(Relating to the Civil Service Commission and Labor-Management in the Federal Service); (aa) Executive Order 13526 and its predecessor orders (Classified National Security Information); (bb) Executive Order 12968 (Access to Classified Information); (cc) 22 CFR Subchapter M (International Traffic in Arms) (applicable to past records); (dd) 40 U.S.C. Chapter 10 (Federal Property and Administrative Services Act (1949)); (ee) 31 U.S.C. (Internal Rev Code); (ff) Pub. L. 99-399, 8/27/86; (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended); (gg) Pub. L. 99-529, 10/24/86 (Special

Foreign Assistance Act of 1986, concerns Haiti) (applicable to past records); (hh) Pub. L. 100-204, Section 155, 12/22/87 (concerns special security program for Department employees responsible for security at certain posts) (applicable to past records); (ii) Pub. L. 100-202, 12/22/87 (Appropriations for Departments of Commerce, Justice, and State) (applicable to past records); (jj) Pub. L. 100-461, 10/1/88 (Foreign Operations, Export Financing, and Related Programs Appropriations Act); (kk) Pub. L. 102-138, 10/28/91 (Foreign Relations Authorization Act, Fiscal Years 1992 and 1993) (applicable to past records); (ll) Pub. L. 107-56, 10/26/2001 (USA PATRIOT Act-Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); (mm) Pub. L. 108-21, 4/30/2003 (PROTECT Act-Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003); (nn) Executive Order 12356 (National Security Information) (applicable to past records); (oo) Executive Order 9397 (Numbering System for Federal Accounts Relating to Individual Persons); (pp) HSPD-12, 8/27/04 (Homeland Security Presidential Directive); (qq) Executive Order 13356, 8/27/04 (Strengthening the Sharing of Terrorism Information to Protect Americans); (rr) P.L. 108-458 (Sect.1016), 12/17/04 (Intelligence Reform and Terrorism Prevention Act of 2004); (ss) 22 U.S.C. 254 (Diplomatic Relations Act); and (tt) 22 U.S.C. 4301 et seq. (Foreign Missions Act).

PURPOSE(S):

The records maintained in State-36, Security Records, capture data related to incidents and threats affecting U. S. Government personnel, U. S. Government information, or U. S. Government facilities world-wide for a variety of legal purposes including Federal and state law enforcement and counterterrorism purposes. The information maintained in Security Records can also be used to determine general suitability for employment or retention in employment, and to grant a contract or issue a license, grant, or security clearance.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The information in the Security Records is used by:

(a) Appropriate Congressional Committees in furtherance of their respective oversight functions;

(b) Department of Treasury; U.S. Office of Personnel Management; Agency for International Development; Department of Commerce; Peace Corps; Department of Defense; Central Intelligence Agency; Department of Justice; Department of Homeland Security; National Counter Terrorism Center; and other Federal agencies inquiring pursuant to law or Executive Order in order to make a determination of general suitability for employment or retention in employment, to grant a contract or issue a license, or grant a security clearance;

(c) Any Federal, state, municipal, foreign or international law enforcement or other relevant agency or organization for law enforcement or counterterrorism purposes: threat alerts and analyses, protective intelligence and counterintelligence information, information relevant for screening purposes, and other law enforcement and terrorism-related information as needed by appropriate agencies of the Federal government, states, or municipalities, or foreign or international governments or agencies;

(d) Any other agency or department of the Federal Government pursuant to statutory intelligence responsibilities or other lawful purposes;

(e) Any other agency or department of the Executive Branch having oversight or review authority with regard to its investigative responsibilities;
(f) A Federal, state, local, foreign, or international agency or other public authority that investigates, prosecutes or assists in investigation, prosecution or violation of criminal law or enforces, implements or assists in enforcement or implementation of statute, rule, regulation or order;
(g) A Federal, state, local or foreign agency or other public authority or professional organization maintaining civil, criminal, and other relevant enforcement or pertinent records such as current licenses; information can be given to a customer reporting agency: (1) In order to obtain information, relevant enforcement records or other pertinent records such as current licenses or (2) To obtain information relevant to an agency investigation, a decision concerning the hiring or retention of an employee or other personnel action, the issuance of a security clearance or the initiation of administrative, civil, or criminal action;
(h) Officials of government agencies in the letting of a contract, issuance of a license, grant or other benefit, and the establishment of a claim;
(i) Any private or public source, witness, or subject from which information is requested in the course of a legitimate agency investigation or other inquiry to the extent necessary to identify an individual; to inform a source, witness or subject of the nature and purpose of the investigation or other inquiry; and to identify the information requested;
(j) An attorney or other designated representative of any source, witness or subject described in paragraph (j) of the Privacy Act only to the extent that the information would be provided to that category of individual itself in the course of an investigation or other inquiry;
(k) A Federal agency following a response to its subpoena or to a prosecution request that such record be released for the purpose of its introduction to a grand jury;
(l) Relevant information may be disclosed from this system to the news media and general public in furtherance of a legitimate law enforcement or public safety function as determined by the Department, e.g., to assist in the location of Federal fugitives, to provide notification of arrests, to provide alerts, assessments or similar information on potential threats to life, health or property, or to keep the public appropriately informed of other law enforcement or Department matters or other matters of legitimate public interest where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy and could not reasonably be expected to prejudice the outcome of a pending or future trial;
(m) State, local, Federal or non-governmental agencies and entities as needed for purposes of emergency or disaster response; and
(n) U.S. Government agencies within the framework of the National Suspicious Activity Report (SAR) Initiative (NSI) regarding foreign intelligence and terrorist threats managed by the Department of Justice.
The Department of State periodically publishes in the Federal Register its standard routine uses that apply to all of its Privacy Act systems of records. These notices appear in the form of a Prefatory Statement. These standard routine uses apply to Security Records, State-36.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:
Hard copy, physical and electronic media.
RETRIEVABILITY:
The system is accessed by individual name or other personal identifiers.
SAFEGUARDS:
All users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Foreign Service and Civil Service employees and those Locally Engaged Staff who handle PII are required to take the Foreign Service Institute (FSI) distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Security Records, a user must first be granted access to the Department of State computer system, and user access is not granted until a background investigation has been completed.
Remote access to the Department of State network from non-Department owned systems is authorized only to unclassified systems and only through a Department-approved access program. Remote access to the unclassified network is configured with the Office of Management and Budget Memorandum M-07-16 security requirements, which include but are not limited to two-factor authentication and time out function.
All Department of State employees and contractors with authorized access have undergone a thorough background security investigation. Access to the Department of State, its annexes and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All paper records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.
RETENTION AND DISPOSAL:
Retention of the records varies depending upon the specific kind of record involved. The records are retired or destroyed in accordance with published records schedules of the Department of State and as approved by the National Archives and Records Administration. More specific information may be obtained by writing to the Director, Office of Information Programs and Services (A/GIS/IPS), SA-2, Department of State, Washington, DC 20522-8100.
SYSTEM MANAGER AND ADDRESS:
For records in the decentralized security records system: Principal Deputy Assistant Secretary for Diplomatic Security and Director, Diplomatic Security Service; Department of State, SA-20, 23rd Floor, 1801 North Lynn Street, Washington, DC 20522-2008 for the Harry S Truman Building, domestic annexes, field offices and missions; Security Officers at respective U.S. embassies, consulates, and missions abroad. For records under the jurisdiction of the Office of Foreign Missions (OFM): Deputy Assistant Secretary and OFM Deputy Director, Harry S Truman Building, 2201 C Street NW, Washington, DC 20520.
NOTIFICATION PROCEDURE:
Individuals who have reason to believe that the Bureau of Diplomatic Security may have security/investigative records pertaining to themselves should write to the Director, Office of Information Programs and

Services, A/GIS/IPS, SA-2, Department of State, Washington, DC 20522-8100. The individual must specify that he/she wishes the Security Records to be checked. At a minimum, the individual must include: name; date and place of birth; current mailing address and zip code; signature; and a brief description of the circumstances that may have caused the creation of the record.

RECORD ACCESS AND AMENDMENT PROCEDURES:

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services (address above).

RECORD SOURCE CATEGORIES:

These records contain information obtained from the individual; persons having knowledge of the individual; persons having knowledge of incidents or other matters of investigative interest to the Department; other U.S. law enforcement agencies and court systems; pertinent records of other Federal, state, or local agencies or foreign governments; pertinent records of private firms or organizations; the intelligence community; and other public sources. The records also contain information obtained from interviews, review of records, and other authorized investigative techniques.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Any exempt records from other agencies' systems of records that are recompiled into this system are also considered exempt to the extent they are claimed as such in the original systems.

Pursuant to 5 U.S.C. 552a (j)(2), records in this system may be exempted from subsections (c)(3) and (4), (d), (e)(1), (2), (3), and (e)(4)(G), (H), and (I), and (f) of the Privacy Act. Pursuant to 5 U.S.C. 552a (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), and (k)(6), records in this system may be exempted from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), (f)(1), (f)(2), (f)(3), (f)(4), and (f)(5).